Principles of Cryptography Problem Sheet 2 Solutions

Dr. Kurunandan Jain[1]†,

[1]Department of Mathematics, Amrita Vishwa, Amrita Campus, Kollam-690525, Kerala, India

(Received xx; revised xx; accepted xx)

1) $y_i \equiv x_i + K_i \mod 26$ $x_i \equiv y_i - K_i \mod 26$

The keystream is a sequence of random integers from $\mathbb{Z}_{26}$

$x_1 = y_1 - K_1 = B - R = 1 - 17 = -16 \equiv 10 \mod 26 = K$ continue this pattern and we get the decrypted text: KASPAR HAUSER

2) We need 128 pairs of plaintext and ciphertext bits in order to determine the keys, s_i is being computed by the formula $s_i = x_i \oplus y_i$ where $i = 0, 1, 2, \cdots 128$

3) See the first and second figures at the end of the answers

c) The two sequences are shifted versions of one another

4) See the third figure at the end of the answers

So the resulting first two output bytes are 1001000011111111

5) $S(x_1) \oplus S(x_2)$=1110 and $S(x_1 \oplus x_2) = 0000$.

They are not equal

b) $S(x_1) \oplus S(x_2)$=1001 and $S(x_1 \oplus x_2) = 1000$.

They are not equal

c) $S(x_1) \oplus S(x_2)$=1010 and $S(x_1 \oplus x_2) = 1101$.

They are not equal

6) $S_1(000000) = 14 = 1110$

$S_2(000000) = 15 = 1111$

$S_3(000000) = 10 = 1010$

$S_4(000000) = 7 = 0111$

$S_5(000000) = 2 = 0010$

$S_6(000000) = 12 = 1100$

$S_7(000000) = 4 = 0100$

$S_8(000000) = 13 = 1101$

$P(S) = D8D8DBBC$

(L_1, R_1) =(0000 0000 D8D8 DBBC)

7) $IP(x)$ maps bit position 57 to position 33, which is position 1 in in R_0

E-Expansion box maps bit position 1 to positions 2 and 48.

Therefore the input to S-boxes are: $S_1 = 010000$ and $S_2 = 000000 = S_3 = S_4 = S_5 = S_6 = S_7$ and $S_8 = 000001$

Two S-boxes get a different input

$P(S)$ =D058 5B9E and thus (L_1, R_1)=80000 0000 D058 5B9E

a) 2 S-boxes get a different input S_1 and S_8

b) According to design criteria, a minimum of 2 bits/bit, thus 4 bits.

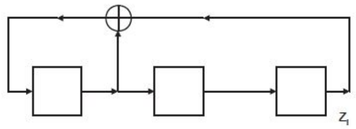
c) See above.

d) 6 bits have changed, 3 from S_1 2 from S_8 and 1 in the left half.

8) See the fourth figure on the last page See the third figure at the end of the answers

9) Multiplying $A(x)$ and $B(x)$ together yields

† Email address for correspondence: kurunandanj@am.amrita.edu

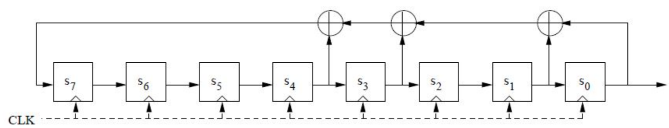


1	0	0	$= Z_0$
1	1	0	$= Z_1$
1	1	1	$= Z_2$
0	1	1	$= Z_3$
1	0	1	$= Z_4$
0	1	0	$= Z_5$
0	0	1	$= Z_6$
1	0	0	$= Z_7 = Z_0$

1. **Sequence 1: z_0 = 0 0 1 1 1 0 1 0 0 1 1 1 0 1 ...**

0	1	1	$= Z_0$
1	0	1	$= Z_1$
0	1	0	$= Z_2$
0	0	1	$= Z_3$
1	0	0	$= Z_4$
1	1	0	$= Z_5$
1	1	1	$= Z_6$
0	1	1	$= Z_7 = Z_0$

2. **Sequence 2: z_0 = 1 1 0 1 0 0 1 1 1 0 1 0 0 1 ...**



1	1	1	1	1	1	1	1	$= Z_0$
0	1	1	1	1	1	1	1	$= Z_1$
0	0	1	1	1	1	1	1	$= Z_2$
0	0	0	1	1	1	1	1	
0	0	0	0	1	1	1	1	
1	0	0	0	0	1	1	1	
0	1	0	0	0	0	1	1	
0	0	1	0	0	0	0	1	
1	0	0	1	0	0	0	0	
1	1	0	0	1	0	0	0	
1	1	1	0	0	1	0	0	
0	1	1	1	0	0	1	0	
0	0	1	1	1	0	0	1	
1	0	0	1	1	1	0	0	
0	1	0	0	1	1	1	0	$= Z_{14}$
0	0	1	0	0	1	1	1	$= Z_{15}$

Multiplication table for $GF(2^3)$, $P(x) = x^3 + x + 1$

$\times$	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	0	0	0	0	0	0	0
1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x	0	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
$x+1$	0	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
x^2	0	x^2	$x+1$	x^2+x+1	x^2+x	x	x^2+1	1
x^2+1	0	x^2+1	1	x^2	x	x^2+x+1	$x+1$	x^2+x
x^2+x	0	x^2+x	x^2+x+1	1	x^2+1	$x+1$	x	x^2
x^2+x+1	0	x^2+x+1	x^2+1	x	1	x^2+x	x^2	$x+1$

$(x^2+1)(x^3+x^2+1) = x^5+x^4+2x^2+x^3+1$

After division we obtain the remainder $x^3 - x^2$ which is the same as x^3+x^2 and thus the answer is $C(x) = x^3+x^2$

b) $(x^2+1)(x+1) = x^3+x^2+1$ after division it's clear the remainder is $C(x) = x^3+x^2+1$